



HEALTH AFFAIRS



HIPAA Security Rule Essentials

TMA Privacy Office

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

Agenda

- HIPAA Security Background
- Key Concepts and Terms
- Security Rule Organization
- Specifics
- Impact
- Compliance

Training Objectives

- Upon completion of this lesson you will be able to:
 - Describe the organization and context of the HIPAA Security Rule
 - Understand HIPAA security standards and implementation specifications
 - Identify tools and other resources that support HIPAA security implementation

HIPAA Implementation Life Cycle



HIPAA Security Background

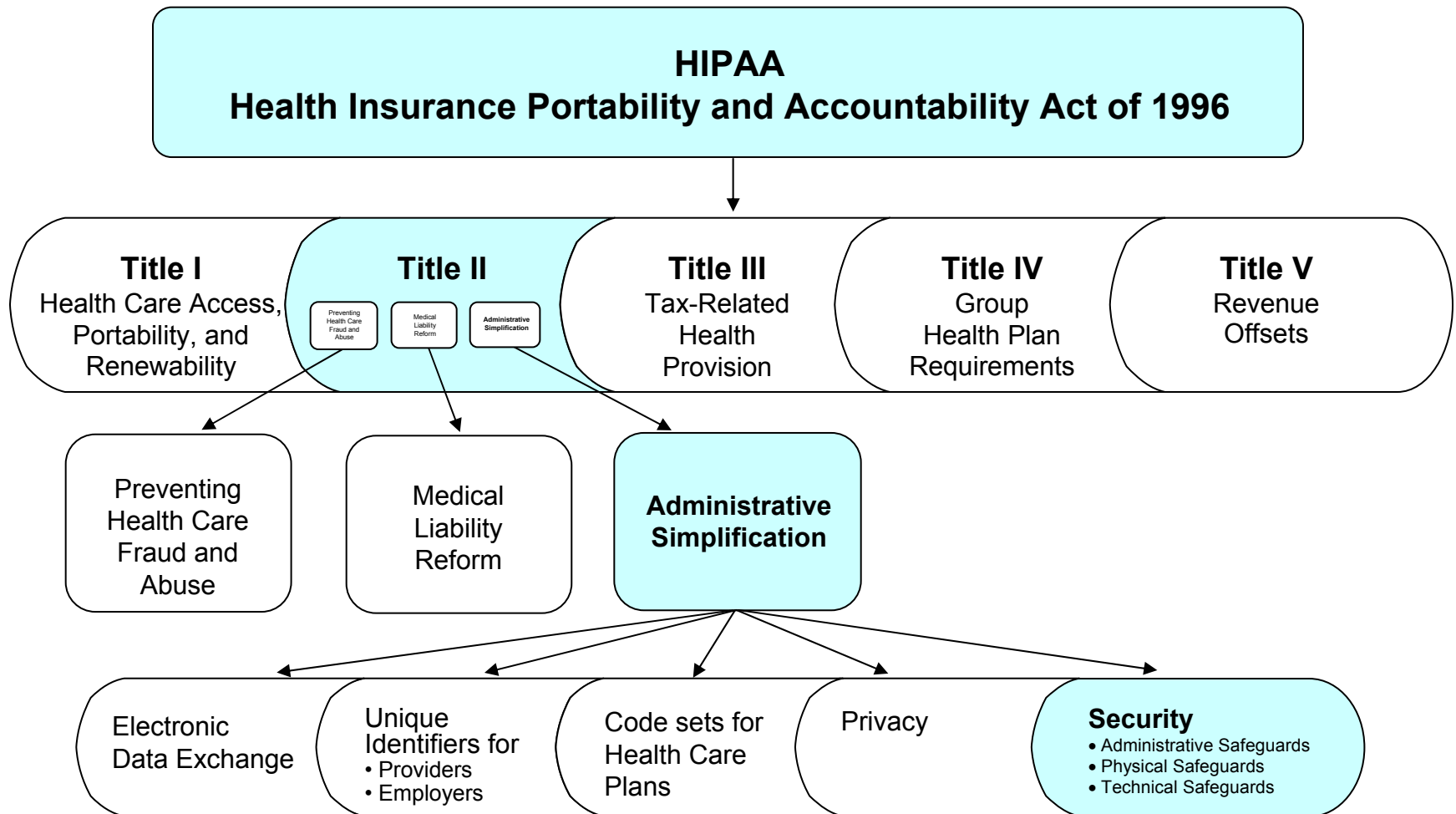
HIPAA Security Rule Background

Objectives

- Upon completion of this module, you will be able to:
 - Describe the purpose and applicability of the HIPAA Security Rule
 - Identify how HIPAA security fits in to the HIPAA Law
 - Explain the differences between HIPAA Privacy versus HIPAA Security

HIPAA Security Rule Background





Where Does This Fit In?



Source: National Institute of Standards and Technology (NIST)

HIPAA Security Rule Background

Applicability of the HIPAA Security Rule

<u>HIPAA ENTITY</u>		<u>MHS ENTITY</u>
Providers who use a covered transaction		MTFs, DTFs, and clinics
Health plans		TRICARE Health Plan
Healthcare clearinghouses		Companies that perform electronic billing on behalf of MTFs
Business associates		Managed care support contractors and other contractors

HIPAA Security Rule Background

Purpose of the HIPAA Security Rule

- To adopt national standards for safeguards to protect the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI)

HIPAA Security Rule Background

Privacy vs Security

Privacy

- HIPAA 1996
- Covered entities
- April, 14 2003
- PHI
- Uses and Disclosures
- Confidentiality
- OCR

Security

- HIPAA 1996
- Covered entities
- No later than April 20, 2005
- EPHI
- Safeguards
- Confidentiality, Integrity, and Availability
- CMS

HIPAA Security Rule Background

Summary

- You should now be able to:
 - Describe the purpose and applicability of the HIPAA Security Rule
 - Identify how HIPAA Security fits in to the HIPAA Law
 - Explain the differences between HIPAA Privacy versus HIPAA Security

Key Concepts and Terms

Key Concepts and Terms

Objectives

- Upon completion of this module, you should be able to:
 - Identify key concepts and terms pertaining to the HIPAA Security Rule and its requirements
 - Identify examples of PHI and EPHI

Key Terms

- HIPAA
- Standards
- Implementation Specifications
- Required
- Addressable
- PHI / EPHI
- Confidentiality, Integrity, Availability
- Compliance

Key Concepts and Terms

HIPAA

- Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191
 - Enacted August 21, 1996
 - Improves portability and continuity of health insurance coverage
 - Improves access to long term care services and coverage
 - Simplifies the administration of health care

Key Concepts and Terms

Standards

- HIPAA Security Rule contains standards and implementation specifications
 - Standards are requirements
 - Eight categories of standards or safeguards:
 - Organizational
 - Security Standards: General Rules
 - Administrative
 - Physical
 - Technical
 - Organizational
 - Policy, Procedures, and Documentation
 - Compliance Dates
 - Standards state what to do, but not how to do it
 - Most standards have implementation specifications

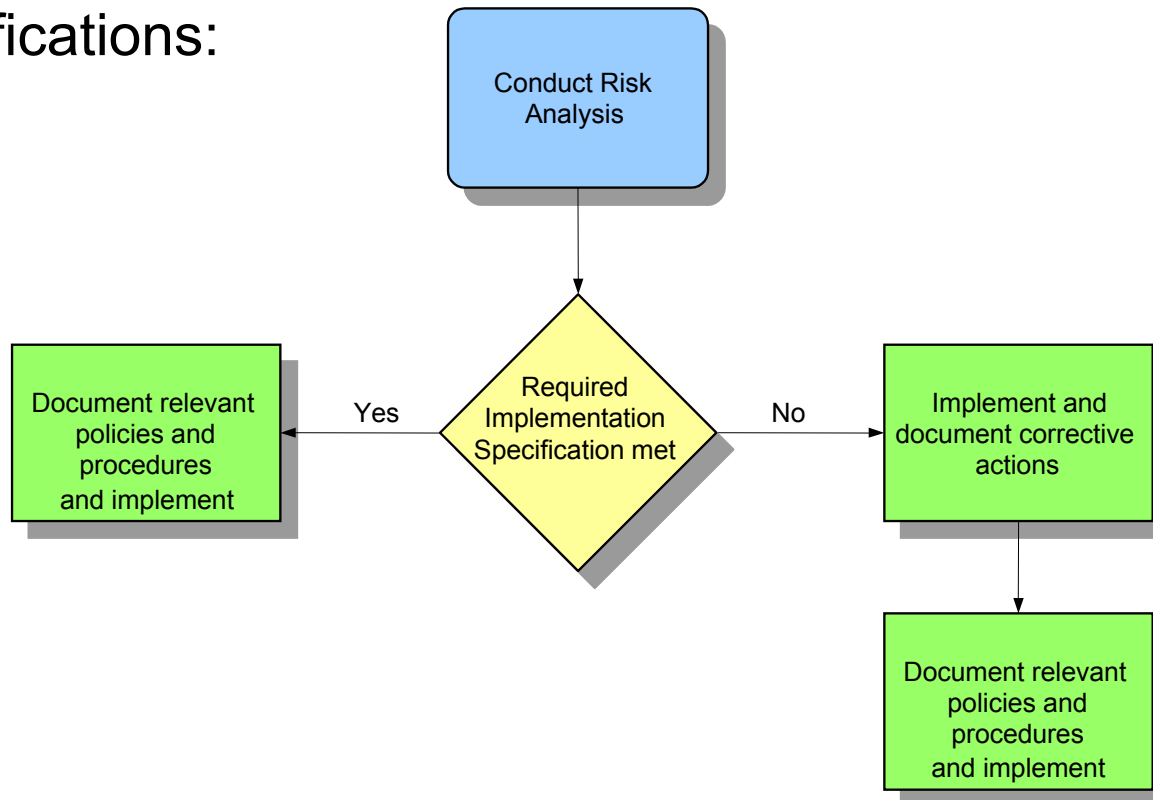
Implementation Specifications

- Implementation specifications support specific standards
- Provide instructions to assist meeting the standards
- Meeting all the implementation specifications does not automatically equate to meeting the standard
- In some cases, a standard itself provides sufficient information for implementation, in which case there is not a distinct implementation specification
- May be “required” or “addressable”

Key Concepts and Terms

Required

- **Required** means that covered entities must carry out the implementation specification at their facility
- For compliance with required implementation specifications:



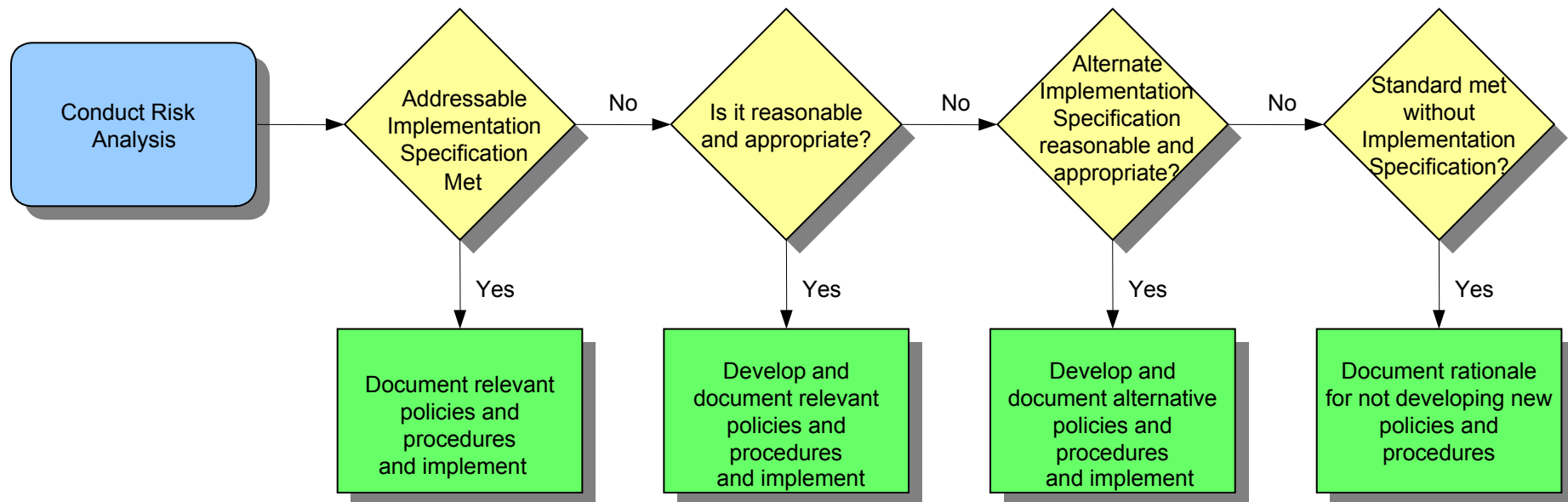
Addressable

- **Addressable** means that covered entities must carry out the implementation specification if it is reasonable and appropriate
- For DoD, only three implementation specifications are addressable

Key Concepts and Terms

Addressable

- For compliance with addressable implementation specifications:



Key Concepts and Terms

PHI / EPHI

- PHI is a sub-set of health information collected from an individual that is created or received by a health provider, health plan, or employer that meets certain criteria
- EPHI is PHI in electronic form that is transmitted or maintained by electronic media
- Not EPHI
 - Traditional fax, voice over telephone, paper copies

Key Concepts and Terms

PHI / EPHI – Criteria

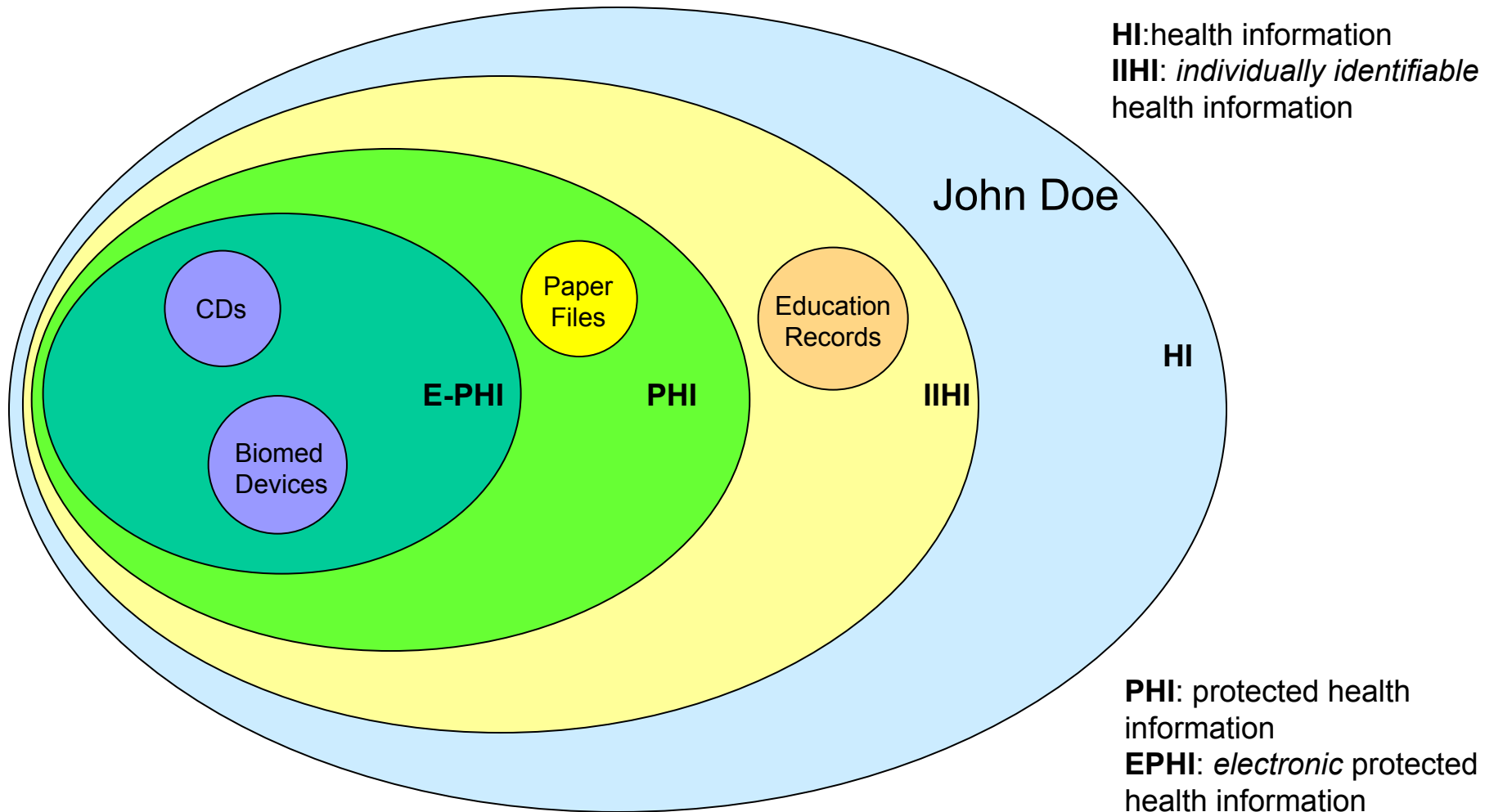
1. Includes past, present, and future information such as:
 - Demographics
 - Health
 - Payment for health services
2. Includes information that can be used to identify the individual

Note: Individually identifiable health information in employment or school records is not PHI



Key Concepts and Terms

The Universe of Health Information



Confidentiality, Integrity, and Availability

- **Confidentiality**: the property that data or information is not made available or disclosed to unauthorized persons or processes
- **Integrity**: the property that data or information has not been altered or destroyed in an unauthorized manner
- **Availability**: the property that data or information is accessible and usable upon demand by an authorized person

Key Concepts and Terms

Compliance

- The Center for Medicare and Medicaid Services (CMS) approach toward HIPAA Security compliance:
 - Complaint driven
 - Voluntary compliance
 - Technical assistance
 - Corrective action plan
 - Progressive steps

Key Concepts and Terms

Summary

- Fax print out of a patient referral for an appointment
- Your medical history on your PDA
- School immunization records
- Digital phone message of appointment reminder
- Printed receipt for payment of medical services
- Diagnosis contained on MRI
- Printed patient medical history

PHI	EPHI	Neither

Key Concepts and Terms

Summary

- Electronic college transcript
- Lab results discussed over the telephone with a doctor
- Social Security Number
- Pathology results saved to CD
- Username and password
- A patient's name and health status emailed by family
- Employee dental billing information on a laptop

PHI	EPHI	Neither

Security Rule Organization

Security Rule Organization

Objectives

- Upon completion of this module, you should be able to identify:
 - HIPAA Security Rule Sections
 - HIPAA Security Requirements Matrix
 - Administrative, physical, and technical requirements (safeguards)
 - Additional Requirements not Listed in the Matrix
 - Standards and Implementation Specifications

HIPAA Security Rule Sections

- Over half of the published rule pertains to the transition from the proposed rule to the final rule, including
 - Comments, analysis, and responses
 - Changes
 - Applicability
- Other sections include
 - Definitions
 - Applicability
 - Regulatory impact analysis

HIPAA Security Rule Sections

- § 164.105 Organizational requirements
- § 164.306 Security standards: General rules
- § 164.308 Administrative safeguards
- § 164.310 Physical safeguards
- § 164.312 Technical safeguards
- § 164.314 Organizational requirements
- § 164.316 Policies and procedures and documentation requirements
- § 164.318 Compliance dates

Appendix A to Subpart C of Part 164 – Security Standards: Matrix

HIPAA Security Requirements Matrix

- Security requirements (safeguards) are listed in a matrix in Appendix A of the Security Rule
- Requirements appear as standards and associated implementation specifications
- Standards and implementation specifications are grouped into Administrative, Physical, and Technical safeguards sections
 - Note: This matrix is not intended to be a complete snapshot of all standards and implementation specifications in the final Security Rule

Security Rule Organization

HIPAA Security Requirements Matrix

- Appendix A to Subpart C of Part 164 - Security Standards: Matrix

Appendix A to Subpart C of Part 164—Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A)
Security Incident Procedures	164.308(a)(6)	Password Management (A) Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Additional Requirements not Listed in the Matrix

- Four sections of standards and implementation specifications are not included in the matrix:
 - § 164.105 Organizational requirements
 - § 164.306 Security standards: General rules
 - § 164.314 Organizational requirements
 - § 164.316 Policies and procedures and documentation requirements
- The first Organizational Requirements section pertains to
 - Hybrid covered entities
 - Affiliated entities
 - Documentation

Additional Requirements not Listed in the Matrix

- **General rules** specify high level requirements for ensuring the confidentiality, integrity, and availability of all EPHI that a CE transmits or processes
- **Organizational requirements** detail requirements for Business Associate Contracts and Group Health Plans
- **Policies and procedures and documentation requirements** specify the implementation and maintenance of policies and procedures to comply with the security requirements

Security Rule Organization

Additional Requirements not Listed in the Matrix

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) *Flexibility of approach.*

(1) Covered entities may use any

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.*

(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the

§ 164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with § 164.306:

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

Standards and Implementation Specifications

- Each section of requirements (or safeguards) contains standards
- Most standards have additional implementation specifications
- The appearance of most standards and implementation specifications follows a consistent pattern

Security Rule Organization

Standards and Implementation Specifications

Physical Safeguards

Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Technical Safeguards (see § 164.312)

Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Security Rule Organization

Standards and Implementation Specifications

§ 164.310 Physical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) **Standard:** *Facility access controls.* Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) **Implementation specifications:**

(i) *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

§ 164.312 Technical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) **Standard:** *Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) **Implementation specifications:**

(i) *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Security Rule Organization

Summary

- You should now be able to identify:
 - HIPAA Security Rule Sections
 - HIPAA Security Requirements Matrix
 - Administrative, physical, and technical requirements (safeguards)
 - Additional Requirements not Listed in the Matrix
 - Standards and Implementation Specifications

Specifics

Objectives

- Upon completion of this module, you should be able to:
 - Identify HIPAA Security Rule standards and implementation specifications
 - Identify the standards and implementation specifications that apply to the DoD
 - Describe which implementation specifications are addressable and which are required by DoD

General Rules

- General Rules
 - Administrative Safeguards
 - Physical Safeguards
 - Technical Safeguards
 - Organizational Requirements
 - Policies and Procedures and Documentation Requirements

Security Standards: General Rules

- The general rules provide the framework for the security standards that:
 - Make the connection between the security standards and the privacy standards
 - Apply to all EPHI the covered entity creates, receives, maintains, or transmits
 - Are designed to be scalable, flexible, and non-technology specific
 - Establish the criteria for compliance
 - Establish requirement for maintenance of safeguards

Administrative Safeguards

- General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

Administrative Safeguards

- Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information

Administrative Safeguards

- Standards
 - Security Management Process
 - Assigned Security Responsibility
 - Workforce Security
 - Information Access Management
 - Security Awareness and Training
 - Security Incident Procedures
 - Contingency Plan
 - Evaluation
 - Business Associate Contracts and Other Arrangements

Standard: Security Management Process

- Implement policies and procedures to prevent, detect, contain, and correct security violations
- Implementation Specifications:
 - Risk analysis
 - Risk management
 - Sanction policy
 - Information system activity review

Standard: Assigned Security Responsibility

- Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity
- Implementation Specifications
 - None



Standard: Workforce Security

- Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to EPHI
- Implementation Specifications:
 - Authorization and/or supervision
 - Workforce clearance procedures
 - Termination procedures

Standard: Information Access Management

- Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements
- Implementation Specifications:
 - Isolating health care clearinghouse functions
 - Access authorization
 - Access establishment and modification

Standard: Security Awareness and Training

- Implement a security awareness and training program for all members of its workforce (including management)
- Implementation Specifications:
 - Security reminders
 - Protection from malicious software
 - Log-in monitoring
 - Password management



Specifics – Administrative Safeguards

Standard: Security Incident Procedures

- Implement policies and procedures to address security incidents
- Implementation Specifications:
 - Response and reporting



Standard: Contingency Plan

- Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI
- Implementation Specifications:
 - Data backup plan
 - Disaster recovery plan
 - Emergency mode operation plan
 - Testing and revision procedures
 - Applications and data criticality analysis

Standard: Evaluation

- Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements
- Implementation Specifications
 - None

Standard: Business Associate Contracts and Other Arrangements

- A covered entity may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate appropriately safeguards the information
- Implementation Specifications:
 - Written contract or other arrangement

Administrative Safeguards Activity

- Design an awareness and training campaign:
 - Choose one administrative safeguard as the focus of the campaign
 - Design a message
 - Identify a target audience
 - Create a communication plan
 - Define the approval process
 - Identify time frames required (mini POA&M)
 - Identify resource requirements
 - Identify opportunities to integrate into existing programs

Specifics

Physical Safeguards

- General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

Specifics

Physical Safeguards

- Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion



Specifics

Physical Safeguards

- Standards
 - Facility access controls
 - Workstation use
 - Workstation security
 - Device and media controls

Standard: Facility Access Controls

- Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed
- Implementation Specifications:
 - Contingency operations
 - Facility security plan
 - Access control and validation procedures
 - Maintenance records

Specifics – Physical Safeguards

Standard: Workstation Use

- Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI
- Implementation Specifications
 - None

Specifics – Physical Safeguards

Standard: Workstation Security

- Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users
- Implementation Specifications
 - None



Standard: Device and Media Controls

- Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility
- Implementation Specifications:
 - Disposal
 - Media re-use
 - Accountability
 - Data backup and storage

Physical Safeguards Activity

- Create a checklist for items to be assessed during a physical security
- What are common vulnerabilities?
- Locations
 - Nursing station
 - Medical Records
 - Computer Room
 - Executive Offices
 - Billing Office
 - Biomed Repair

Technical Safeguards

- General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

Specifics

Technical Safeguards

- Technical safeguards are the technology, as well as the policies and procedures for its use, that protect EPHI and control access to it. The technical safeguards are designed to protect EPHI being created, processed, stored, or transmitted



Technical Safeguards

- Standards
 - Access controls
 - Audit controls
 - Integrity
 - Person or entity authentication
 - Transmission security

Standard: Access Control

- Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights
- Implementation Specifications:
 - Unique user identification
 - Emergency access procedure
 - Automatic logoff (A)
 - Encryption and decryption (A)

Specifics – Technical Safeguards

Standard: Audit Controls

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI
- Implementation Specifications
 - None

Specifics – Technical Safeguards

Standard: Integrity

- Implement policies and procedures to protect EPHI from improper alteration or destruction
- Implementation Specifications:
 - Mechanism to authenticate EPHI

Standard: Person or Entity Authentication

- Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed
- Implementation Specifications
 - None

Standard: Transmission Security

- Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network
- Implementation Specifications:
 - Integrity controls
 - Encryption (A)

Organizational Requirements

- General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

Organizational Requirements

- Organizational requirements are formalized agreements such as business associate contracts and other arrangements that provide assurances that business associates will appropriately safeguard EPHI that is created, received, maintained or transmitted on behalf of the MHS

Organizational Requirements

- Standards
 - Business associate contracts or other arrangements
 - Requirements for group health plans

Standard: Business Associate Contracts or Other Arrangements

- The contract or other arrangement between the covered entity and its business associate must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii), as applicable
- Implementation Specifications:
 - Implement safeguards that protect EPHI
 - Ensure that any agent to whom it provides EPHI agrees to protect it
 - Report to the covered entity any security incident of which it becomes aware
 - CE may terminate a BA that has violated contractual terms
 - If a business associate is required by law to perform a function or activity on behalf...
 - The covered entity may omit from its other arrangements authorization...

Policies and Procedures and Documentation Requirements

- General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

Policies and Procedures and Documentation Requirements

- The standards to implement the policies and procedures specified in the HIPAA Security Rule and meet the documentation requirements

Policies and Procedures and Documentation Requirements

- Standards
 - Policies and Procedures
 - Documentation

Standard: Policies and Procedures

- Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements
- Implementation Specifications
 - None

Specifics- Policies and Procedures and Documentation Requirements

Standard: Documentation

- Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment
- Implementation Specifications
 - Time limit: retain applicable documentation of policies, procedures, actions, activities, assessments for 6 years
 - Availability: make documentation available to involved persons
 - Updates: update documentation when changes affect security of EPHI

Specifics

Summary

- You should now be able to:
 - Identify HIPAA Security Rule standards and implementation specifications
 - Identify the standards and implementation specifications that apply to the DoD
 - Describe which implementation specifications are addressable and which are required by DoD

Impact

Objectives

- Upon completion of this module, you should be able to:
 - Describe the organizational impact of HIPAA Security compliance, including
 - Who is affected
 - Where the HIPAA Security Rule is applicable
 - When compliance must be established
 - How to establish and maintain compliance

Who is affected?

- Covered entities include:
 - MTFs
 - DTFs
 - Intermediate commands (HSOs, Regional Commands, etc)
 - TMA
 - Operational units
 - Reserve forces when serving on active duty

Where is the HIPAA Security Rule Applicable?

- Anywhere the workforce is active
 - MTFs
 - Home
 - Field
 - On travel

Compliance Date

- When does HIPAA Security implementation begin?
 - Now
- When is the mandated deadline for compliance?
 - No later than April 20, 2005

How to Establish and Maintain Compliance?

- To correctly implement the security standards, each covered entity must:
 - Assess potential risks and vulnerabilities to EPHI
 - Develop, implement, and maintain appropriate security measures given those risks
 - Document those measures and keep them current

Implementing HIPAA Security is meant to be flexible and scalable

Impact Summary

- You should now be able to:
 - Describe the organizational impact of HIPAA Security compliance, including
 - Who is affected
 - Where the HIPAA Security Rule is applicable
 - When compliance must be established
 - Why an organization must comply
 - How to establish and maintain compliance

Compliance

Compliance Objectives

- Upon completion of this module, you should be familiar with:
 - Components to establishing and maintaining compliance with HIPAA Security
 - Process
 - Methods
 - Tools
 - Roles and responsibilities
 - Assurance

Process – Risk Analysis

- Risk Analysis is the key to
 - Understanding what must be protected
 - Identifying potential risks and vulnerabilities
 - Initiating Risk Management

Process – Risk Management

- Risk Management, which includes risk analysis, is the process of
 - Assessing risk
 - Mitigating risk
 - Monitoring risk
- Important: risk management is a continuing process – not a one time event

Process – Risk Management Relevance to HIPAA

- Risk analysis determines the following key components to establishing HIPAA Security compliance:
 - The security risks involved in your organization's operations
 - The degree of response to security risks
 - Whether the addressable implementation specifications are reasonable and appropriate
 - Security measures to apply within your particular security framework
- Your ability to assess your state of compliance is greatly improved with risk analysis and a process for managing the data

Compliance Methods

- Methods to assist in establishing and maintaining compliance include
 - Gap / Compliance Assessment
 - Risk Assessment / Management
 - Database Management
 - Reporting

Compliance Tools

- Tools include those provided by TMA
 - HIPAA BASICS™ Compliance Tool
 - HIPAA Training Tool (LMS)
 - PHI Management Tool (PHIMT)
 - OCTAVE™

Roles and Responsibilities

- Successful compliance with HIPAA Security requires clearly defined and assigned roles and responsibilities to ensure
 - Accountability
 - Responsibility
 - Applicability

Roles and Responsibilities

- HIPAA Security Rule requirement for the appointment of a security official
 - Assignment letter for Security Officer
 - Roles and responsibilities
 - Policy Implementation, Oversight, Auditing and Compliance
 - Education, Training and Communication
 - Integration Activities

Roles and Responsibilities

- Other individuals who are part of the compliance initiative include:
 - Commander
 - Chief Information Officer (CIO)
 - Privacy Officer
 - Physical Security Officer
 - Information Security Manager/Officer
 - MTF Analysis and Implementation Team (MISRT)
 - Incident response team

Roles and Responsibilities

- Roles and responsibilities exist throughout the organization, including individuals who are
 - Full-time employees
 - Senior management
 - Part-time employees
 - Contractors
 - Vendors

Compliance Assurance

- Compliance is established and maintained by implementing business practices including
 - Measuring success
 - Identifying areas of improvement
 - Preparations and contingencies
 - Communication

Compliance Summary

- You should now be familiar with:
 - Components to establishing and maintaining compliance with HIPAA Security
 - Process
 - Methods
 - Tools
 - Roles and responsibilities
 - Assurance

HIPAA Security 101

Summary

- You should now be able to:
 - Describe the organization and context of the HIPAA Security Rule
 - Understand HIPAA security standards and implementation specifications
 - Identify methods, tools, and other resources that support HIPAA Security implementation

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- [www.tricare.osd.mil/tmaprivacy/HIPAA.cfm](http://www.tricare.osd mil/tmaprivacy/HIPAA.cfm)
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA security representatives



HEALTH AFFAIRS



Please fill out your critique

Thanks!

